INL/CON-12-24570
PREPRINT

Safeguards-By-Design: Guidance and Tools for Stakeholders

SHAPE 2012

M. Schanfein
S. Johnson

February 2012

The INL is a
U.S. Department of Energy
National Laboratory
operated by
Battelle Energy Alliance

Safeguards-By-Design: Guidance and Tools for Stakeholders

INL/CON-12-24570

Authors: M. Schanfein, Idaho National Laboratory, S. Johnson, Tucker Creek Consulting

Abstract

Effective implementation of the Safeguards-by-Design (SBD) approach can help meet the challenges of global nuclear energy growth by designing facilities that have improved safeguardability and reduced safeguards-related life cycle costs. The ultimate goal of SBD is to implement effective and efficient safeguards that reduce the burden to both the facility operator and the International Atomic Energy Agency (IAEA).

Since 2008, the U.S. National Nuclear Security Administration's Next Generation Safeguards Initiative's (NGSI) Safeguards-By-Design Project has initiated multiple studies and workshops with industry and regulatory stakeholders, including the State Regulatory Authority (SRA) and the IAEA, to develop relevant documents to support the implementation of SBD. These "Good Practices Guides" describe facility and process design features that will facilitate implementation of effective nuclear material safeguards starting in the earliest phases of design through to final design and construction. These guides, which are in their final editorial stages, start at a high level and then narrow down to specific nuclear fuel cycle facilities such as Light Water Reactors, Generation III/IV Reactors, High Temperature Gas Cooled Reactors, and Gas Centrifuge Enrichment Plants. Most recently, NGSI has begun development of a facility safeguardability assessment (FSA) approach to assist the designer. This paper will review the current status of these efforts and provide some examples of these documents.

Introduction

From the earliest days of international safeguards inspections by the IAEA, inspectors have been challenged by facilities that were not designed to allow for efficient and effective safeguards inspections. These challenges grew as more States brought the Non-Proliferation Treaty into force and their existing facilities came under IAEA inspection. The lack of material access and operational transparency made implementation of safeguards costly and inefficient. Examples of some of these issues include material process hold up, unmeasureable material, lack of secure locking fixtures on storage areas, and inaccessible areas for design information verification.

In the 1980s, a revolution in IAEA international safeguards technology started with the installation of the first unattended monitoring systems (UMS) at the Tokai Reprocessing Plant in Japan and at the Darlington CANDU reactor in Canada. The old model of inspectors periodically performing inspections at nuclear facilities with manual instrumentation and verifying nuclear material on a statistical sampling basis to draw conclusions, an approach that interfered with plant operations, would soon be supplemented and replaced, where practical, with automated technologies that could continuously monitor while a facility operated. When UMS was

considered for a facility, a cost benefit analysis was done. A positive decision was made when the cost of the UMS was recovered in 3 years or less compared to the cost of inspector presence.

This was a transition that brought the promise of more effective and efficient safeguards for both the IAEA and the State. The safeguards sensors could not only continuously monitor operations but could do so in areas of a nuclear facility where inspectors could not enter due to high radiation and other safety limitations. And with this came a dramatic reduction in inspector presence and the collection of higher quality data. However, as the number of facilities needing these systems grew the introduction of modern IAEA unattended and remote monitoring systems would have to be retrofitted into these existing facilities. Such an activity, while required by existing circumstances, was costly, time consuming, had considerable impact on the operator, and resulted in less than effective safeguards due to the necessary trade-offs under these less than ideal conditions.

The most basic needs of an IAEA monitoring system include: physical space, mains power, and a data transmission backbone (wired or wireless). Even without detailed IAEA design criteria for safeguards monitoring systems, the ability to provide access to stable secure power and data transmission throughout a nuclear facility would address some of the most costly aspects of retrofitting in safeguards monitoring systems and allow flexibility for future safeguards technologies. One might refer to these most basic needs as the Minimum Safeguards equipment Infrastructure Set (MSIS).

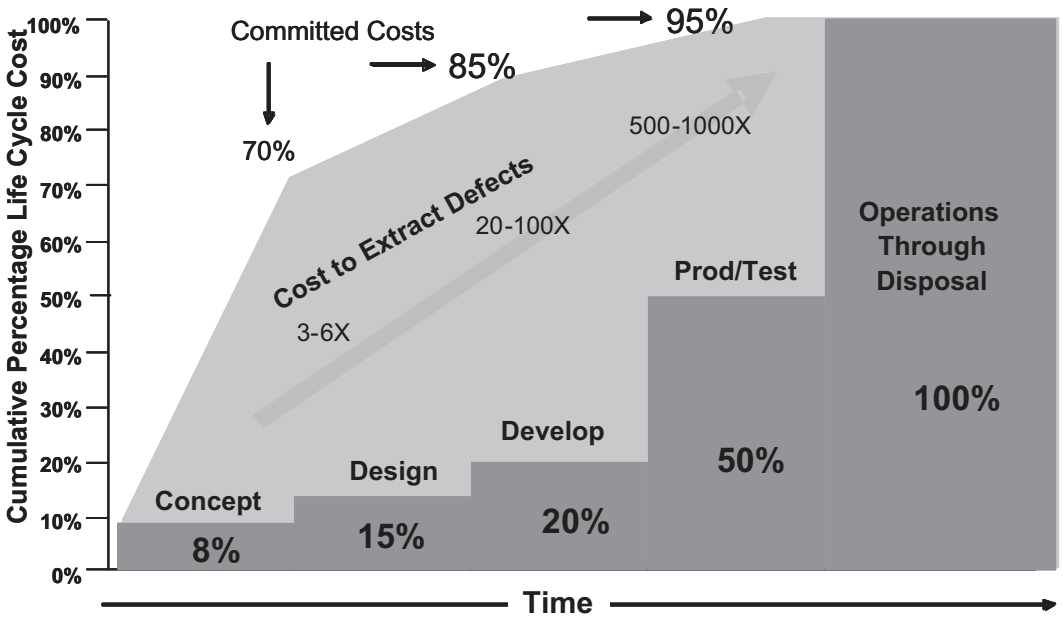
The use of unattended monitoring systems supports a new model for inspectors, where the reduction of in-facility time spent by inspectors allows inspectors to concentrate on other aspects of safeguards (see the appendix for some example components/systems). Most recently, the IAEA focus on the State Level Concept (SLC) has required more headquarters time for the inspectors. The SLC not only includes IAEA analysis of the data from inspections at declared facilities but also includes, for example, open source analysis, environmental sampling, satellite surveillance, and member State-supplied information. By considering all of this information, the IAEA draws conclusions on both the correctness and completeness of a State's expanded declaration.

Project Considerations

Project managers have always tried to minimize errors in design, as the cost to extract "defects" in any process increases dramatically the later the solution comes in construction projects. US Defense Acquisition project experience may be a useful guide here to provide a frame of reference to consider the cost impacts of failing to consider safeguards early in the design phases of facility construction (Figure 1). Correcting or retrofitting a facility to address safeguards needs is costly.

Over the next couple of decades as nuclear processing technologies of enrichment and reprocessing reached outside the weapons States, resulting in the construction

of commercial scale facilities, there was renewed interest in fully integrating safeguards at early stages in a facility's conceptual design. This concept of designing safeguards into the facility in the earliest stages includes not only the identification of IAEA equipment, but also operational parameters and procedures to accommodate IAEA verification requirements.



Committed Life Cycle Costs Against Time
Figure 1[1]

This would take into consideration: inspector access for other activities such as design information verification where facility construction and capabilities are verified against the declared design/functionality; minimization of alternate nuclear material pathways to reduce verification needs; clear material balance area boundaries where potential losses and gains can be verified; access to all nuclear material streams and storage locations for verification; and continuity of knowledge of nuclear materials and operations.

With the introduction in the U.S. of the Next Generation Safeguards Initiative (NGSI), under the leadership of the Office of Non-proliferation and International Security and along with the worldwide nuclear renaissance, the need to formalize a process to address the installation of safeguards from the earliest stages in a nuclear facility's design became an important focus. In 2008, NGSI initiated efforts to understand and explore the aspects of facility project management within the context of nuclear facilities for the purpose of incorporating the Safeguards-By-Design (SBD) concept.

[1] Source: Defense Acquisition University 1993

Safeguards-By-Design: The Basics

SBD is a design approach whereby international and State safeguards are fully designed into the process of a nuclear facility, from initial planning through design, construction, and operation. The best analogy to draw in order to capture the entire concept is the relationship between safety and the nuclear fuel cycle. Safety is designed into nuclear facilities as part of a State's regulatory requirement and has been since the start of the commercial nuclear fuel cycle (Figure 2). The consideration of safety in nuclear facility design is one that has evolved over decades as the industry and regulators gained experience. Basic high level examples include no positive power coefficient, multilayered containment, emergency core cooling system, provision for decay heat removal, and emergency core injection system. Then, the question is, "How do you institutionalize SBD in the commercial nuclear fuel cycle?"

Figure 2

Keeping in mind the target of routine, global use of the SBD approach as a long-term objective, the required support structure might include three main pillars[2]:

- *Requirements Definition*, (for SBD process and nuclear facility design and construction)
- *Design Process* (including project coordination of all related activities and systems engineering)
- *Technology* (to meet IAEA needs) & *Methodology* (for design and testing if the design meets requirements/acceptance criteria)

Institutionalization or normalization of SBD should be accomplished through outreach, education, training, demonstration, negotiations (among key stakeholders), standardization, and deployment.

SBD Good Practices Guides

Under the Safeguards-by-Design Project of NGSI, good practice guides have been prepared ranging from general guidance to facility-specific guidance; they provide information that designers will need to support the SBD concept and accomplish SBD objectives. A brief listing of these guides and their focus areas follows:

Generic

- *Safeguards by Design General Guidance*, LA-UR-09-05802, Rev 1, 2009,
- *SBD: Safeguards Requirements and Success Criteria*, LA-UR-09-08160, Rev 0, Nov 2009,
- *Implementing the SBD Process*, INL/EXT-09-17085, Rev 0, Oct 2009, INL
- *SBD: Safeguards Evaluations for Trade Studies*, LA-UR-10-01035, Rev 1, Feb 2010,
- *Review and Analysis of Development of "Safety by Design" Requirements*, PNNL-18848, Oct 2009

Facility Specific

Reactors

- *Safeguards by Design (SBD): Safeguards Guidance for GEN III/III+ Light Water Reactors,* LA-UR-11-00226 Revision 1
- *Safeguards Guidance Document for Designers of Commercial Nuclear Facilities: International Nuclear Safeguards Requirements and Practices for High Temperature Gas Reactors (Pebble Fuel HTGRs),* INL/EXT-10-18438
- *Safeguards Guidance Document for Designers of Commercial Nuclear Facilities: International Nuclear Safeguards Requirements and Practices for High Temperature Gas Reactors (Prismatic Fuel HTGRs),* INL/EXT-10-17981

[2] Implementing the Safeguards-by-Design Process, Bjornard, Bean, Durst, Hockert, Morgan, INL/EXT-09-17085, October 2009

Conversion, Enrichment and Spent Fuel Storage

- *Implementing Safeguards-by-Design at Natural Uranium Conversion Plants*, ORNL/TM-2011/July 2011
- *Implementing Safeguards-by-Design at Gas Centrifuge Enrichment Plants*, ORNL/TM-2010/87
- *Safeguards-by-Design: Guidance for Independent Spent Fuel Storage Installations (ISFSI),* INL/LTD-11-22940 Revision 0

Lessons-learned Reports

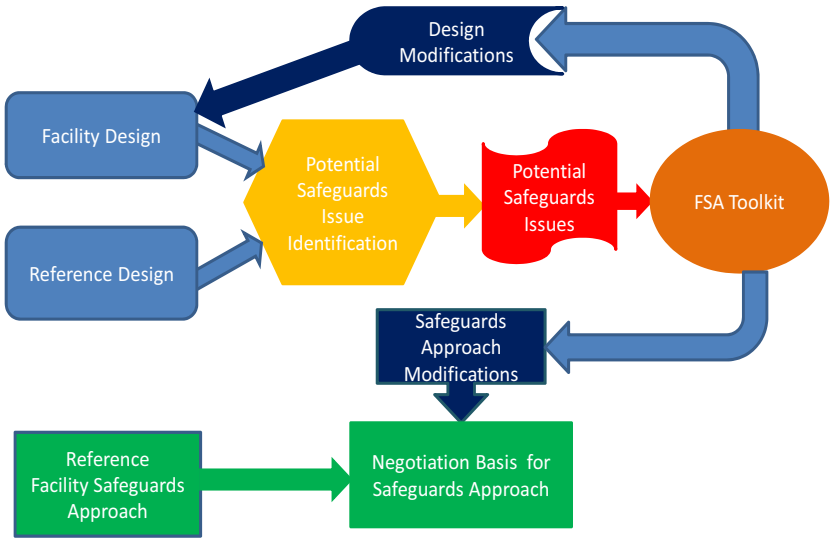
Important relevant lessons from more recent nuclear facility construction were also captured in the following reports.

- *Safeguards-by-Design: The Canadian Experience*, IAEA-CN-184/219
- *Safeguards by Design - experiences from new nuclear installation – Finland*, IAEA-CN-184/24
- *URENCO's experience of "Safeguards by Design" in gas centrifuge enrichment plants*, NNSA/NGS Meeting, Washington, DC. 14-15 Dec 2010
- *Designing and Operating for Safeguards: Lessons Learned From the Rokkasho Reprocessing Plant* (RRP), PNNL-19626
- *EURATOM's "Safeguards During Construction" Approach at AREVA's MELOX Facility*, NNSA/NGS Meeting, Washington, DC. 14-15 Dec 2010
- *Advanced Safeguards for New Fuel Cycle Facilities – Developments and Recommendations*, PNNL-18185
- *Application of Safeguards-by-Design to a Reactor Design Process*, International Atomic Energy Agency Symposium on International Safeguards, November, 2010, IAEA-CN-184/10

In order to identify differences between a conceptual facility design and the design of a similar facility with an IAEA-accepted safeguard approach, NGSI is developing a Facility Safeguardability Assessment (FSA) Process and Toolkit[3] to provide a simple process for designers. This process (Figure 3) is designed to identify potential changes in safeguards approaches and measures needed to accommodate the new design. This process could also be used to evaluate the effect of facility design modifications on an existing safeguards approach. The intention is to provide a simple tool to help the designer become engaged in international safeguards by design, identify safeguards issues or challenges, and then find resources (the toolkit) that might be used to help address the issues. The SBD good practice guides for a particular type of facility would be one such resource. In the end, of course, the

[3] Facility Safeguardability Assessment Report, PNNL-20829

IAEA will negotiate its safeguards approach to a specific facility in a specific country based on a number of considerations, especially in the state-level-concept, and the State Regulatory Authority will play a key role in this negotiation process. FSA and SBD should help the designer participate more effectively in this process, and help ensure that facility design accommodates the safeguards measures the IAEA will apply.



FSA Process

Figure 3

The FSA approach is designed to enable the owner/operator/designer to draw the attention of the SRA and IAEA to design changes and features that may have potential IAEA safeguards impact early in the design process. It is important to note that an FSA may also identify intrinsic improvements in facility safeguardability as a result of design changes that may result in a more efficient and cost effective safeguards approach.

The FSA process employs a screening tool in the form of questions to identify aspects of the new design that may create potential safeguards issues when compared to applicable facilities. Five focused question areas have been generated to date. At the highest level is the Facility Safeguardability Assessment Screening Questions (Table 1), followed by more focused screening questions whose details are not given here but can be found in the referenced document. These focus areas include: Physical Inventory Verification, Interim Inventory/Verifications, Inventory Change Measurement, and Other Strategic Points.

Based upon a comparison of new facility designs with current IAEA safeguarded designs, this tool can enable designers and their safeguards experts to identify

Table 1 Facility Safeguardability Assessment Screening Questions

Facility Safeguardability Assessment Screening Questions	
1. Does this design differ from the comparison design / process in ways that have the potential to create additional diversion paths or alter existing diversion paths?	Yes / No
1.1. Does this design introduce nuclear material of a type, category, or form that may have a different significant quantity or detection time objective than previous designs/processes (e.g., mixed oxide rather than low enriched uranium, irradiated vs. unirradiated or bulk rather than items)?	Yes / No
1.2. Does this design layout eliminate or modify physical barriers that would prevent the removal of nuclear material from process or material balance areas, e.g., circumventing a key measurement point (KMP)?	Yes / No
1.3. Does this design obscure process areas or material balance area (MBA) boundaries making containment/surveillance or installation of verification measurement and monitoring equipment more difficult?	Yes / No
1.4. Does this design introduce materials that could be effectively substituted for safeguarded nuclear material to conceal diversion?	Yes / No
2. Does this design differ from the comparison design in a way that increases the difficulty of design information examination (DIE) and verification (DIV) by IAEA inspectors?	Yes / No
2.1. Does the design incorporate new or modified technology? If so, does the IAEA have experience with the new or modified technology?	Yes / No
2.2. Are there new design features with commercial or security sensitivities that would inhibit or preclude IAEA inspector access to equipment or information?	Yes / No
2.3. Do aspects of the design limit or preclude inspector access to, or the continuous availability of, Essential Equipment for verification or testing?	Yes / No
2.4. Are there aspects of the design that would preclude or limit IAEA maintenance of Continuity of Knowledge (CoK) associated with design verification during the life of the facility.	Yes / No
3. Does this design/process differ from the comparison design / process in a way that makes it more difficult to verify that diversion has not taken place?	Yes / No
3.1. Does this design lessen the efficiency of physical inventory taking (PIT) by the operator or the effectiveness of physical inventory verification (PIV) by the IAEA?	Yes / No
3.2. Does this design impair the ability of the operator to produce timely and accurate interim inventory declarations or for the IAEA to perform timely and accurate Interim Inventory Verification (IIV)?	Yes / No
3.3. Does this design impede timely and accurate inventory change (IC) measurements and declarations by the operator and verification by the IAEA?	Yes / No
3.4. Does this design impede the introduction of or reduce the usefulness of Other Strategic Points (OSP) within a Material Balance Area (MBA)?	Yes / No
4. Does this design differ from the comparison design in ways that create new or alter existing opportunities for facility misuse or make detection of misuse more difficult?	Yes / No
4.1. Does this design differ from the comparison facility / process by including new equipment or process steps that could change the nuclear material being processed to a type, category, or form with a lower significant quantity or detection time objectives?	Yes / No
4.2. Should the comparison facility safeguards approach employ agreed upon short-notice visits or inspections, measurements, or process parameter confirmations, would this design preclude the use of or reduce the effectiveness of these measures?	Yes / No
4.3. Do the design and operating procedures reduce the transparency of plant operations (e.g., availability of operating records and reports or source data for inspector examination or limited inspector access to plant areas and equipment)?	Yes / No

potential safeguards issues in the earliest part of the design process when there is more design flexibility to resolve them. The more the design of the facility departs from the design of existing facilities, or is a unique, one-of-a-kind facility, the value of comparison to existing facilities to identity what might be unique to the new facility will diminish. Nonetheless, the screening tool questions are designed to help focus the designer and its safeguards experts on safeguards issues that might be posed in any facility. For its part, the IAEA is developing a set of high level principles and guidelines for SBD that is expected to be published in 2012.

Conclusions

Safeguards-by-Design (SBD) for new nuclear facilities has the promise to enable efficient and effective safeguards in an economical way, while raising operational efficiency. But the path to institutionalize SBD within the existing culture will take time to incorporate and will only be successful by concerted efforts on the part of all stakeholders: nuclear facility owner/operator, designer, State regulatory authority, and the IAEA.

Application of SBD to State Regulatory Authority requirements is another consideration that could be a major contributor to the success of the SBD process for international safeguards. The FSA process is expected to be adaptable to most regulatory, project management, and engineering environments, and applicable to many nuclear facility types. Much work remains to achieve international consensus and broad adoption of SBD for such an application.

This paper has laid out a broad perspective including some historical context, some examples of IAEA facility material access, transparency, and safeguards equipment types and challenges to both orient those new to the SBD concept and inform the reader on the ongoing development of guides and tools that can formalize the implementation of SBD. Early inclusion of requirements and identification of beneficial design features are key to SBD and the safeguardability of today's and tomorrow's nuclear fuel cycle.

Appendix

Unattended Safeguards Equipment

An unattended monitoring system (UMS) is any automated monitoring system comprised of a single or multiple set of sensors, designed so that it can maintain continuity of knowledge about the content and location of all nuclear material of interest in a facility 24 hours a day and 365 days a year. The concept of Continuity of Knowledge (COK) can take many forms, from tracking spent fuel bundles or assemblies to performing a quantitative analysis on cans of mixed oxide fuel. The intent is that the system can provide the necessary assurance for the IAEA to draw rapid, comprehensive, and definitive conclusions that nuclear material is not being diverted from peaceful use.

Depending on the safeguards approach, UMS could be permanently installed in a nuclear facility. It is computer-based for data retrieval either on-site or remotely and may use a variety of sensors such as optical, radiation, pressure, temperature, flow, vibration, and electromagnetic fields to collect qualitative or quantitative data. Because of the need to assure that all data is authentic, all external components are installed in tamper indicating enclosures and all data transmissions are encrypted and/or authenticated.

The use of UMS was particularly true in Japan as they pursued not only the complete nuclear fuel cycle with the construction of the first large scale reprocessing facility under comprehensive safeguards but also the development of a fully automated fuel fabrication manufacturing plant. Automation of every aspect of a process forced consideration for automation of safeguards. This automation of safeguards went beyond simple perimeter monitoring systems to being directly designed into the process, sometimes resulting in the need for the expanded use of Joint-Use Equipment. These are systems used by both the operator and the IAEA and include the necessary design features to assure that the IAEA can independently verify items while maintaining authentication of the instrument and the data it generates. This joint approach reflects a cost effective and efficient approach to safeguards where space and operational limitations are paramount.

The following are some examples of typical UMS components and cabinets (Figures 1 - 6):

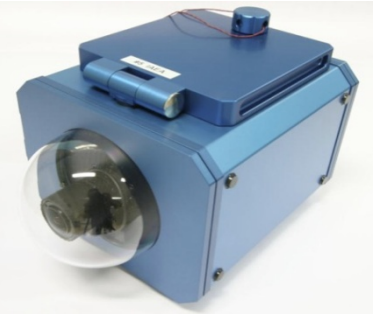


Figure 1 - Surveillance camera: Optical sensor to record visual images

Figure 2 – Entrance Gate Monitor Detector: Neutron collar to quantify plutonium in MOX fresh fuel assembly

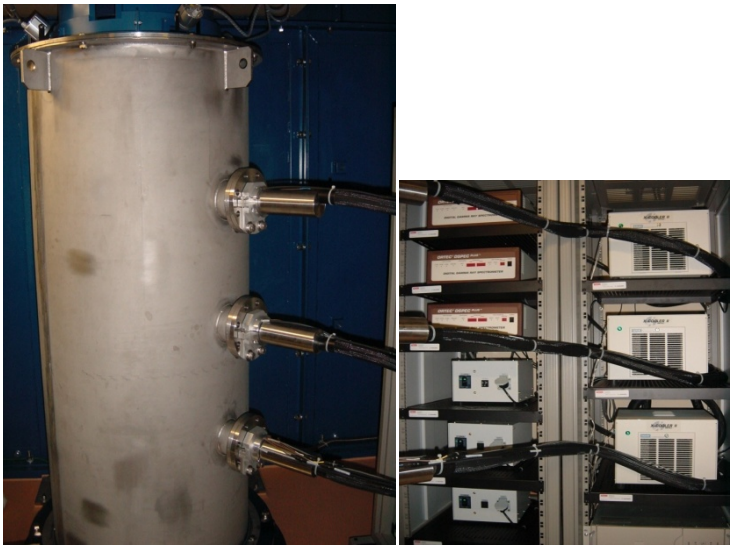


Figure 3 – Plutonium Assay Canister System: Neutron counter and gamma isotopic spectroscopy to quantify plutonium in MOX power cans

Figure 4 – Thermo-hydraulic Power Monitor: Installation of ultrasonic flow sensors on primary core coolant loop of research reactor to calculate Pu in core fuel

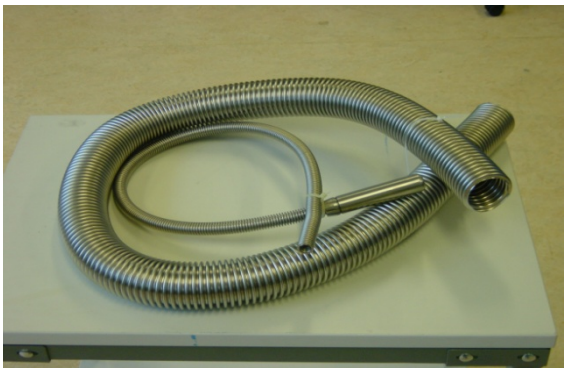


Figure 5 – Tamper Indicating Conduit: Used to secure sensor cables from sensor to data collection cabinet

Figure 6 – Standard Instrumentation Cabinet: Typical components include data collect modules attached to sensors, local uninterruptable power supply, data collect computer, air conditioner, network

All of these systems are designed for high reliability and robustness. In order to maintain that reliability, these systems are typically connected to Class II facility power systems (secondary safety systems) that provide long-term back up power (diesel generators and/or battery back-up) in case of mains failure. With designed in provisions to meet at least the minimum safeguards equipment infrastructure set (MSIS) comprised of: reliable power, data transmission (wired or wireless) from sensors and cabinets, and space, allows for significant cost reductions in the installation. Significantly better would be consideration of this equipment in the earliest stages of facility design.